Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-23 (canceled)

24. (new) An apparatus for storage of data comprising:

means for storing copies of a plurality of data items,

means for generating at the end of a predetermined period of time, a data file comprising hash values of each data item created and/or stored during that time,

means for generating a single hash value of said data file, and

means for transmitting said single hash value to a remote location for storage or publication of the single hash value or publication of data representative thereof.

25. (new) The apparatus according to claim 24 wherein said data file comprises a hash value of each of the data items created or stored during said predetermined period of time together with one or more of a file name, a path name, the file size and a time-stamp in relation to each data item.

26. (new) The apparatus according to claim 24 wherein at said remote location, a second data file is created comprising said single hash value and one or more additional data items relating to said single hash value, and a single hash value, and a single hash value, said second data file being stored or published.

27. (new) A method of storing and authenticating data, comprising the steps of:

storing copies of a plurality of data items,

generating at the end of a predetermined period of time, a data file comprising hash values of each data item created and/or signed during that time,

generating a single hash value of said data file, and

transmitting said single hash value to a remote location for storage of the single hash value or publication of the single hash value or publication thereof (or data representative thereof.

28. (new) The method of claim 27, further comprising the steps of:

creating a second data file comprising said single hash value and one or more data items relating thereto, and

creating a single hash value of said second data file for storage or publication.

29. (new) The method of claim 27, further comprising the steps of:

retrieving a stored set of data items for a predetermined time period,

generating a data file comprising the hash values of each of said data items, and

comparing one or more of said hash values with the corresponding hash value or values sin the data file generated in claim 27 to determine whether or not they match.

30. (new) The method of claim 29, further comprising the steps of:

generating a single hash value of the data file generated in claim 29, and comparing it with the corresponding single hash value generated in claim 27, to determine whether or not they match.

31. (new) An apparatus for transmitting data between first and second end users via an information technology communications network,

said first end user comprising means for encrypting a data item using a first identifier and transmitting said encrypted data item to said second end user,

said second end user comprising means for receiving said encrypted data item and transmitting an acknowledgement signal to said first end user,

said first end user further comprising means for encrypting said first identifier using a second identifier and transmitting said encrypted first identifier to said second end user in response to receipt of said acknowledgement signal,

said second end user further comprising means for requesting and receiving said second identifier in response to receipt of said encrypted first identifier, and

means for decrypting said first identifier using said second identifier and for decrypting said data item using said first identifier.

32. (new) The apparatus of claim 31, wherein the second identifier is stored remotely from said first and second end users.

33. (new) The apparatus of claim 32 wherein the second identifier is stored by a third party.

34. (new) The apparatus of claim 32 wherein said second identifier is transmitted to said remote storage location by said first end user in response to commencement of a data transfer transaction thereby.

35. (new) The apparatus of claim 34, wherein the transaction embodied by transmission of a second identifier to the remote storage location is time stamped.

36. (new) The apparatus of claim 31, wherein a request for the second identifier is sent to said remote storage location, the request being in the form of the encrypted data item or an encrypted version of the first identifier.

37. (new) The apparatus of claim 31, wherein the data item is encrypted using a symmetric key and the first identifier or key is encrypted using an asymmetric key.

38. (new) The apparatus of claim 31, wherein the acknowledgement signal comprises an encrypted or compressed version of the original data item.

39. (new) The apparatus of claim 38 wherein the encrypted or compressed version of the original data item is a has value thereof.

40. (new) A method for transmitting data between first and second end users via an information technology communications network, comprising the steps of:

encrypting by the first end user a data item using a first identifier and transmitting said encrypted data item to said second end user,

receiving by said second end user said encrypted data item and transmitting an acknowledgement signal to said first end user,

said first end user encrypting said first identifier using a second identifier and transmitting said encrypted first identifier to said second end user in response to receipt of said acknowledgement signal,

said second end user requesting and receiving said second identifier in response to receipt of said encrypted first identifier, decrypting said first identifier using said second identifier and decrypting said data item using said first identifier.

41. (new) An apparatus for verifying by a second end user the authenticity of use of an identifier by a first end user, the apparatus comprising:

means for identifying the communication of a data item encrypted using or otherwise including an identifier unique to said first end user from said first end user to said second end user across an information technology communications network,

means for accessing, in response to such identification, storage means containing information relating to one or more valid recent events or transactions relating to said identifier which have occurred across said information technology communications network,

means for obtaining confirmation from said first end user that at least one of said recent events or transactions is valid, and

means for preventing further use of said identifier in the event that such confirmation is not received.

42. (new) A method for verifying by a second end user the authenticity of use of an identifier by a first end user, the method comprising the steps of:

identifying the communication of a data item encrypted using or otherwise including an identifier unique to said first end user from said first end user to said second end user across an information technology communications network,

accessing, in response to such identification, storage means containing information relating to one or more valid recent events or transactions relating to said identifier which have occurred across said information technology communications network,

obtaining confirmation from said first end user that at least one of said recent events or transactions is valid, and

preventing further use of said identifier in the event that such confirmation is not received.